UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,928	03/31/2000	Ulhas S Warrier	10559-148001/P7973	2224

20985 7590 12/04/2003

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/04/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/539,928	WARRIER ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This action is responsive to communication: original application filed 31 March 2000.

2. Claims 1- 24 are currently pending in this application. Claims 1, 9, 17, and 21 are independent claims.

Oath/Declaration

3. The oath is objected to as being informal. It lacks authentication by a diplomatic or consular officer of the United States; 37 CFR 1.66(a). This informality can be overcome either by forwarding the original oath to the appropriate officer for authentication or by filing either a declaration under 37 CFR 1.68, or a new properly authenticated oath under 37 CFR 1.66. The new oath or declaration must properly identify the application of which it is to form a part, preferably by application number and filing date in the body of the oath or declaration. If, however, authentication of the original oath is desired, applicant should request return of the oath for this purpose. Such request must be accompanied by an order for a copy of the oath to be retained in the file until the properly authenticated oath is returned. After the oath has been authenticated, it should be returned promptly to the Patent and Trademark Office. See MPEP §§ 602.01 and 602.02.

It does not include the notary's signature.

It does not include the notary's seal and venue.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1-4, 7, 8 and 17** rejected under 35 U.S.C. 102(e) as being anticipated by Flint et al. U.S. Patent No. 6,453,419 (hereinafter '419).

6. **As to independent claim 1,** "A method of managing a network session" is disclosed in '419 col. 2, line 11-13 "According to another aspect of the present invention, an access control mechanism is described in computer network";

- "delivering policies from a server to a remote system that has predetermined configuration information" is shown in '419 col. 2, lines 16-17 "The access control mechanism includes a plurality of regions, including a first and second region, one or more services bridging said first and second region";

- "establish a secure connection between the server and the system" is taught in '419 col. 2, lines 17-18 "bridging said first and second region, access control rules which define security policy";

- "regulating activities in the system based on at least one of the set of policies and the predetermined configuration information" is disclosed in '419 col. 2 lines 13-17

"control mechanism ... first and second region, access control rules which define a security policy".

7. **As to dependent claim 2,** "The method of claim1 wherein regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria" is disclosed in '419 col. 5, lines 1-4 "In one embodiment, filter node 72 can force user authentication or encryption, can use filters to block particular WWW connections or can filter the connection to see if it contains Java or ActiveX content".

8. **As to dependent claim 3,** "The method of claim 2 wherein the rejection criteria include the predetermined static configuration information" is disclosed in '419 col. 2, lines 29-33 "According to yet another aspect of the present invention, a system and method of limiting transfer between networks comprises the steps of defining a to-from set, wherein the to-from set lists a source network and a destination network".

9. **As to dependent claim 4,** "The method of claim 2, wherein the rejection criteria include the set of policies" is disclosed in '419 col. 1 lines 6-8 "The present invention is a system and method of implementing a security policy, comprising the steps of providing a plurality of access policies".

10. **As to dependent claim 7,** "The method of claim 1 further comprising updating the set of policies" is disclosed in '419 col. 4, lines 16-18 "This is all the code that implements the rules themselves in the kernel including: building, modifying, deleting, and querying the rules".

11. **As to dependent claim 8,** "The method of claim 1 further comprising: detecting data packets from the regulated activities; and rejecting the data packets from the regulated activities" is disclosed in '419 col. 3 lines 48-53 "For each connection attempt, the Firewall checks it against the defined access rules. The rule that matches the characteristics of the connection request is used to determine whether the connection should be allowed or denied."

12. **As to independent claim 17,** "A network system, comprising: first and second devices" is disclosed in '419 col. 2, lines 29-33 "According to yet another aspect of the present invention, a system and method for limiting transfers between networks comprises the steps of defining a to-from set, wherein the to-from set lists a source network and a destination network";

- "the first device is adapted to: deliver a set of policies to the second device" is taught in '419 col. 2, lines 16-17 "one or more services bridging said first and second region, access control rules define a security policy";

- "the second device is adapted to: detect data packets from unauthorized activities" is disclosed in '419 col. 3, lines 48-49 "Firewall 34 protects regions from unauthorized access through the use of access rules";

- "reject the data packets from the unauthorized activities" is shown in '419 col. 3, lines 48-53 "For each connection attempt, the Firewall checks it against the defined access rules. The rule that matches the characteristics of the connection request is used to determine whether the connection should be allowed or denied".

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. **Claims 5-6** rejected under 35 U.S.C. 103(a) as being unpatentable over '419 as applied to independent claim 1 above, in view of Green et al., U.S. Patent No. 6,003,084 (hereinafter '84).

15. **As to dependent claims 5,** the exact terminology of "The method of independent claim 1 wherein regulating the activities comprises providing a session layer adapted to reject unauthorized data packets based on context such as user and application form" **is not used in '419 however** "If a security violation is detected, a meaningful application specific protocol response can be created from context information captured during the session" is taught in '84 col. 2, lines15-18. It would have been obvious to incorporate the teachings of '84 into '419, which discloses a system, and method of implementing an access control mechanism to maintain security in a computer network policy. One of ordinary skill in the art would have been motivated to perform such a modification because the OSI protocol layer structure is an important element to maintain network security as stated in '84 (col. 6 lines 55 et seq. thru col. 8 lines 66 et seq.) "To protect themselves from attacks by malicious outsiders,

organizations are turning to mechanisms for increasing network security". (col. 8 lines 66 et seq.) "Finally, to complete proxy processing and ensure that only specific OSI application data is being passed though the session, the proxy software continually examines the OSI application level protocols within the data frames".

16. **As to dependent claims 6,** "The method of claim 1 wherein regulating the activities comprises: providing a session layer adapted to reject unauthorized data packets based on context information" is taught in'84 col. 2, lines15-18 "If a security violation is detected, a meaningful application specific protocol response can be created from context information captured during the session" and in '84 col. 12, lines 14-19 "The network communication session manager of claim 2 wherein the plurality of distinct layers includes a presentation layer, a session layer and a transport layer and wherein the connection manager rejects a remote responding entity by generating a response at the presentation layer, the session layer, and the transport layer";

- "providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies" is disclosed in '419 col. 5, lines 1-4 "In one embodiment, filter node 72 can force user authentication or encryption, can use filters to block particular WWW connections or can filter the connection to see if it contains Java or ActiveX content".

17. **Claims 9-16** rejected under 35 U.S.C. 103(a) as being unpatentable over '419 in view of '84.

18. **As to independent claim 9,** "based on at least one of the set of policies and the predetermined configuration information" is disclosed in '419 col. 2 lines 13-17 "control

mechanism ... first and second region, access control rules which define a security policy". **The exact terminology of** "An article comprising a computer-readable medium which stores computer-executable instruction for managing a network session, the instructions causing a computer to: receive a set of policies from a server in a remote system having predetermined configuration information; establish a secure connection between the server and the system; and manage activities" **is not used in '419 however** "A storage medium having a computer program stored thereon for causing a suitably programmed system to ensure communications between a requesting application entity and a serving application entity, by performing the following steps when such program is executed on the system: responding to an entity requesting a connection to the serving application entity; establishing a transparent session connection operable at a plurality of layers, between the system and the requesting entity; monitoring, at a plurality of distinct protocol layers, communication from the requesting entity for conformance to a selected communication protocol; and relaying communication between the requesting entity and the serving entity responsive to the conformance to the selected communication protocol, and further wherein the relay operates at or below the plurality of distinct protocol layers" is disclosed in '419 col. 13, lines 25-43. It would have been obvious to incorporate the teachings of '84 into '419, which discloses a system, and method of implementing an access control mechanism to maintain security in a computer network policy. One of ordinary skill in the art would have been motivated to perform such a modification because a network security application can be transferred by any computer-readable means, as stated in '84 (col. 7,

lines 51 et seq.) "It should be noted that disk drive 120 is used herein to represent various storage medium by which the computer program 210 may be stored and distributed".

19. **As to dependent claims 10, 11, 12, 13, 14, and 15** these claims are dependent on claim 9 and contain the same claims as indicated in claims 7, 2, 3, 4, 5, and 6 respectively and are rejected under the same rationale as stated above in paragraphs 10, 7, 8, 9, 15, and 16.

20. **As to dependent claim 16,** "The article of claim 9, further comprising instructions to: detect unauthorized data packets from the unauthorized activities; and reject the unauthorized data packets from the unauthorized activities" is disclosed in '419 col. 3 lines 48-53 "For each connection attempt, the Firewall checks it against the defined access rules. The rule that matches the characteristics of the connection request is used to determine whether the connection should be allowed or denied."

21. **Claims 18-20** rejected under 35 U.S.C. 103(a) as being unpatentable over '419 as applied to independent claim 17 above, in view of '84.

22. **As to dependent claim 18,** the exact terminology of "The system of claim 17 further comprising a network stack" **is not disclosed in '419 however** "The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports" is taught in '84 col. 5 lines 36-39. It would have been obvious to incorporate the teachings of '84 into '419, which discloses a system, and method of implementing an access

control mechanism to maintain security in a computer network policy. One of ordinary skill in the art would have been motivated to perform such a modification because of the complexity of the required security as indicated in '84 (col. 4, lines17 et seq.) "Because of the complexity of the required service elements and the upper layers of the OSI stack, application layer gateways for OSI services tend to be implementations of the application server themselves sometimes with limited functionality".

23. **As to dependent claim 19,** *"The system of claim 18, wherein the network stack comprises: a policy engine connected to the first device ... a policy store connected to the policy engine"* is disclosed in'84 col. 5 lines 36-39 "The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports"

- *"a socket interceptor connected to the policy engine"* is disclosed in '419 col. 3 lines 48-53 "For each connection attempt, the Firewall checks it against the defined access rules. The rule that matches the characteristics of the connection request is used to determine whether the connection should be allowed or denied."

- *"a packet guard connected to the policy engine*" is disclosed in '419 col. 5, lines 1-4 "In one embodiment, filter node 72 can force user authentication or encryption, can use filters to block particular WWW connections or can filter the connection to see if it contains Java or ActiveX content".

24. **As to dependent claim 20,** "The system of claim 17, the first device further comprising instruction to monitor the system for the intervening process" is disclosed in '84 col. 5 lines 36-39 "The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports".

25. **Claims 21-24** rejected under 35 U.S.C. 103(a) as being unpatentable over '419 in view of '84, and in further view of Cunningham et al., U.S. Patent No. 6,219,786 (hereinafter '786).

26. **As to independent claim 21,** "A network stack" is taught in '84 col. 5 lines 36-39 "The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports"

- *"comprising: a policy engine"* is disclosed in'84 col. 5 lines 36-39 "The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports";

- The exact terminology of the below text in italics was not indicated in the combination of teachings from '419 and '84:

- *"a policy store adapted to interact with the policy engine and store a set of policies from the policy engine; "* is disclosed in '786 col. 4 lines 13-17 "the access rules are preferably stored as a rules base, which may be centralized if there is more than

one node that provides access management. Alternatively, the rules base is configured at a single site, but then automatically distributed to each access control point on the network";

- *"a socket interceptor coupled to the policy engine"* is shown in '786 col. 1, lines 54-56 "These gateways are "choke points, through which network traffic that is to be controlled must flow" and '786 col. 6, lines 8-9 "an access control module 34 is installed on the firewall 16 in order to form a gateway access control station (GACS)"

- *"a packet guard coupled to the policy engine"* is disclosed in '786 col. 3 lines 21- 34 "access control to resources of a network by collecting and assembling data packets of a specific transmission, so as to enable identification of information from raw data packets at the lowest level to application-level data at the top-most level. In terms of the standardized model referred to as the International Standards Organization (ISO) model, the data packets are assembled to determine not only the lower-layer information from the headers of the packets, but also the uppermost Application Layer (i.e., Layer 7) contextual information. Access rules are then applied to determine whether the specific transmission is a restricted transmission".

- It would have been obvious to incorporate in '786 into the combination of teachings from '419 and '84, which discloses a system, and method of implementing an access control mechanism to maintain security in a computer network policy with network stack and OSI information. One of ordinary skill in the art would have been motivated to perform such a modification because as indicated in '786 a policy store maintains the flexibility for the network see '786 (col. 3 lines 16 et seq.) "What is needed

is a method and system for providing access control to resources of a network in a manner that is flexible, scalable and relatively easy to administer".

27. **As to dependent claim 22,** "The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard" is disclosed in '786 col. 2 lines 58-63 "By monitoring all packets, the system detects occurrences in which a device attempts to "disguise" itself by first training with an authorized source address and then sending a packet with an unauthorized source address."

28. **As to dependent claim 23,** "The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server" is disclosed in '786 col. 4 lines 13-17 "the access rules are preferably stored as a rules base, which may be centralized if there is more than one node that provides access management. Alternatively, the rules base is configured at a single site, but then automatically distributed to each access control point on the network."

29. **As to dependent claim 24,** "The network stack of claim 23 further comprising a configurable management process adapted to reconfigure the network stack"

- "having instruction to: receive policies in the policy engine from the policy server" is disclosed in '786 col. 4 lines 13-17 "the access rules are preferably stored as a rules base, which may be centralized if there is more than one node that provides access management. Alternatively, the rules base is configured at a single site, but then automatically distributed to each access control point on the network";

- "use the socket interceptor to detect and reject data packets from unauthorized users and applications" " is shown in '786 col. 1, lines 54-56 "These gateways are "choke points, through which network traffic that is to be controlled must flow" and '786 col. 6, lines 8-9 "an access control module 34 is installed on the firewall 16 in order to form a gateway access control station (GACS)";

- "provide the packet guard with context information about the unauthorized users and applications" is disclosed in '786 col. 3 lines 21- 34 "access control to resources of a network by collecting and assembling data packets of a specific transmission, so as to enable identification of information from raw data packets at the lowest level to application-level data at the top-most level. In terms of the standardized model referred to as the International Standards Organization (ISO) model, the data packets are assembled to determine not only the lower-layer information from the headers of the packets, but also the uppermost Application Layer (i.e., Layer 7) contextual information. Access rules are then applied to determine whether the specific transmission is a restricted transmission".

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm Monday - Thursday and alternating Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone

number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

NORMAN M. WRIGHT
PRIMARY EXAMINER